NATIONAL INSTITUTE OF TECHNOLOGY ROURKELA

Comparison of Zero Knowledge Authentication Protocols

By

SUBHASISH PARAMANIK
(110CS0371)

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE

REQUIREMENTS FOR THE DEGREE OF

Bachelor of Technology

In
Department of Computer Science & Engineering

Under the guidance of
Prof. A. K. Turuk

May 2014

Certificate

This is to certify that **Mr. Subhasish Paramanik** has carried out his project on the topic of **Comparison of Zero Knowledge Authentication Protocols** under my supervision for the award of the degree in Bachelor in Technology. To the best of my knowledge the matter in this thesis has not been submitted by any other college/university for the partial fulfillment of the requirements for any Degree or Diploma.

.

Prof. Ashok Kumar Turuk

Dept. of Computer Science and Engineering

National Institute of Technology, Rourkela

Acknowledgement

I convey my gratitude to my guide Prof. Ashok Kumar Turuk for giving me the opportunity to do my project under his guidance and mentorship. Like a true mentor, he has always motivated and inspired me throughout my entire project work, without which I couldn't have achieved my goal.

.

I want to thank all the other faculty members of Department of Computer Science and Engineering, NIT Rourkela for their perennial support during the entire duration of my project. I would like to thank my friends for their support all throughout this project.

Last but not the least, I express my sincere gratitude to the Almighty and my parents for their blessings without which I would have never managed to complete my work.

Date:

Place:

Subhasish Paramanik

110cs0371

Department of Computer Science & Engineering

N.I.T Rourkela

Author's Declaration

I hereby declare that all the work contained in this report is my own particular work unless otherwise recognized. Also, all of my work has not been previously submitted for any scholarly degree. All sources of quoted information have been recognized by method of appropriate references.

Subhasish Paramanik
NIT Rourkela

Abstract

A Zero knowledge Authentication is a protocol which takes place between two parties called the Claimant and the Verifier. In the Zero Knowledge Authentication, anything which may increase the danger of confidentiality of the secret is not revealed by one party, which is called the claimant. The claimant simply has to prove the other part called the verifier that it knows a secret, without telling it. The interactions are designed not to give or reveal any secret. After interchanging messages, the verifier can only know that the claimant does or doesn't have the secret. The result which is found out is simply a yes/no situation that has only single bit of information. Here the three important protocols of Zero knowledge Authentication have been implemented, which are Fiat-Shamir protocol, Fiege-Fiat Shamir protocol and Guillou- Quisquater protocol and their performances are compared.

Contents

List of Figures

Chapter 1

Introduction

We are living in the age of information. Every aspect's information has to be kept, because information has a value. As an asset it has to be secured. To be secured, we need to hide information from unauthorized access (Confidentiality), protect it from unauthorized change (Integrity) , and to make it available to an authorized entity whenever it is needed (Availability). In the present world most of the communication takes place via unsecured channel, so it is open to various attacks. Building a secured channel is very expensive. While sending data we need to take care of mainly these goals.

- Confidentiality: Security from unknown persons
- Integrity: Security from information change
- Authentication: Assurance of identification of entity/person

These are the primary security goals a message passing system must satisfy for a successful communication. In the past, cryptography mainly concerned with the confidentiality factor. The most application of cryptography were in the department of defense or other organization to collect and report secret information on an enemy or competitor. Integrity verification, user authentication, digital signatures etc. have been added to the confidentiality.

1.1 Entity Authentication:

It is basically a technique that is used by one party to prove the identity of another party. An entity may be a client, a process or a person. The entity whose identity has to be known is called a Claimant while the entity which proves the identity of the claimant is called the Verifier. When A tries to prove the identity of B, B is called the claimant and A is called the Verifier.

Difference with Message Authentication:

We generally differentiate message authentication from entity authentication by 2 ways.

- Message authentication is not a real time authentication; while entity authentication does. In the message authentication when A sends a message to B, the claimant may or may not be in the process while they are communicating. Contrary to message authentication, in the entity authentication there is not a message which is involved until B is authenticated by A.
- Message Authentication simply authenticates one message, as the process has to repeat it for each new message. Entity authentication authenticates the claimant for the entire session.

1.2 Types of Entity Authentication:

In claimant verification, the claimant must be identified by the verifier. This verification can be done with one of the three kind of techniques: anything known, anything possessed, anything inherited.

1. Anything Known: A secret known to claimant, which is checked by the verifier. Example- a pin, a key (secret) etc.
2. Anything Possessed: This is used to prove the claimant's identity. Example- a credit card, driving license.
3. Anything Inherited: Inherent characteristics of the claimant are described here. Example- normal signatures, biometric characteristics.

There are 3 types of Entity Authentication.

1. Password based Authentication
2. Challenge Response Authentication
3. Zero Knowledge Authentication

1.2.1 Password based Authentication:

This is the simplest and the most used entity authentication technique, in which case the claimant has an idea about the password. A password is used when a user needs the system to be accessed. Each user has a public user identification, and a password, which is the private key. This authentication scheme is divided into 2 types.

1.2.1.1 Fixed Password: A fixed password is used repeatedly for every access. Several schemes have been built, one upon the other.

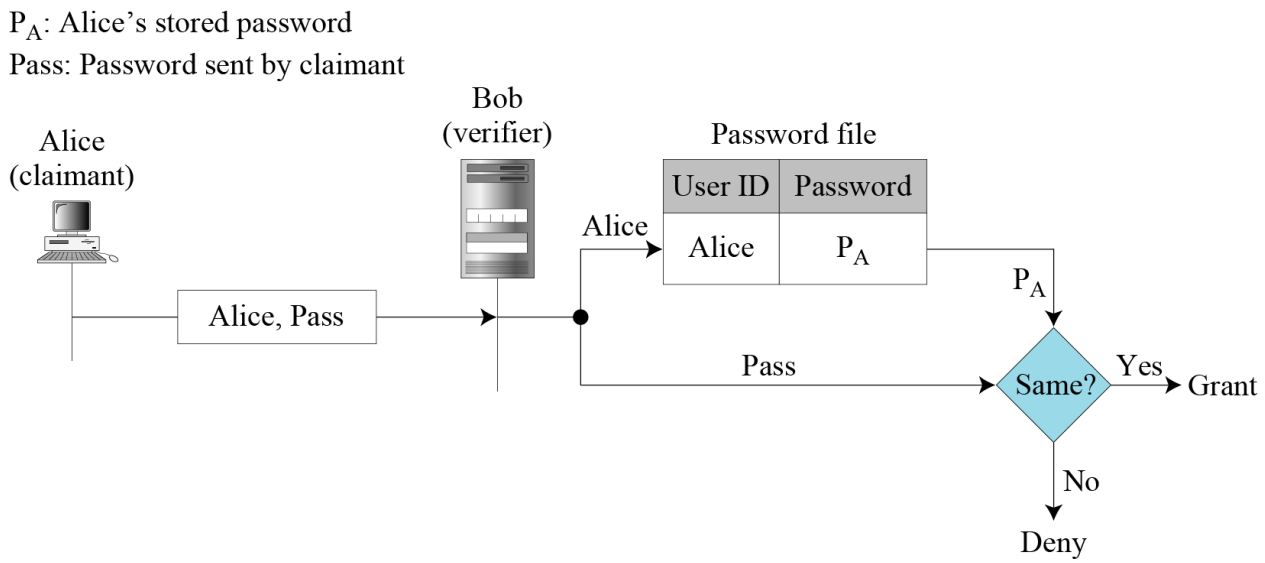


Fig.1.1 User ID and Password file

1.2.1.2 One-time Password: This is used only once for gaining access. This kind of password makes eavesdropping and salting useless.

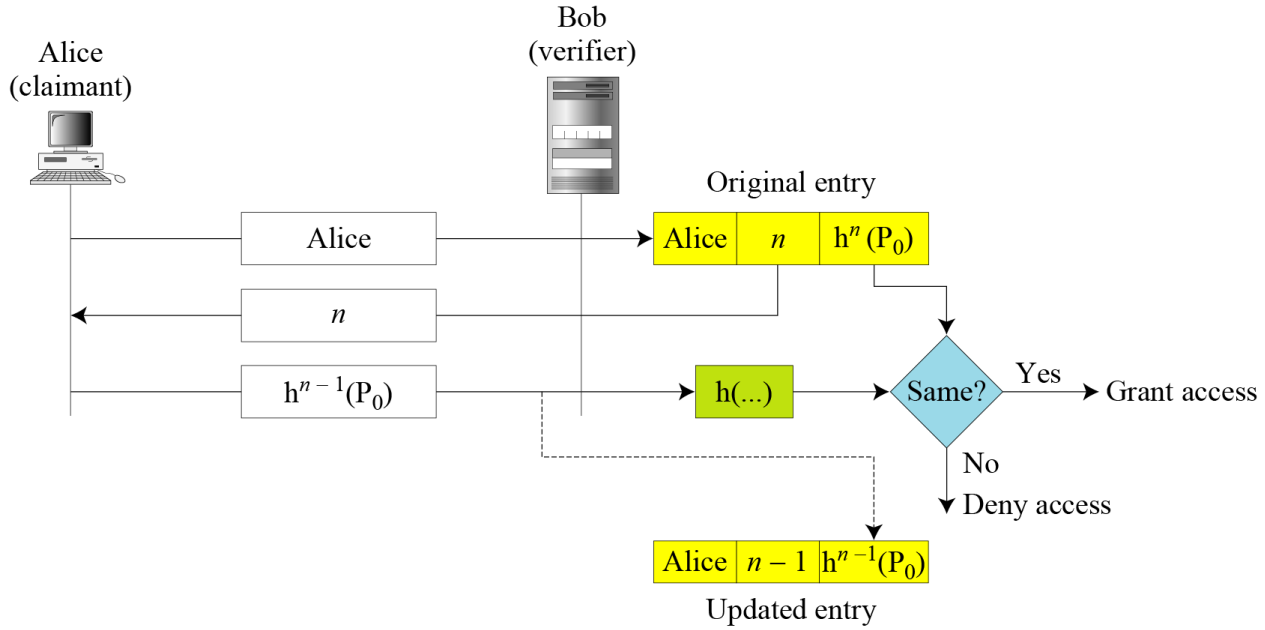


Fig.1.2 Lamport one-time password

1.2.2 Challenge Response Authentication

In password based authentication, the claimant demonstrates to prove a secret. However because the claimant reveals this secret, it is open to various attacks. In the Challenge Response authentication, the claimant has to prove that it has the knowledge of the password without letting the verifier know. In other words the claimant doesn't send the secret to the verifier, the latter can search for it and find it.

The Challenge is basically a time-varying value like any random number. The claimant applies a function to the challenge and sends the result, which is termed as a response, to the verifier. The response shows that the claimant has knowledge about the secret.

It can be done by four methods.

1. Using a Symmetric-key cipher
2. Using keyed-hash functions
3. Using Asymmetric-key cipher
4. Using Digital Signatures

1.2.2.1 Using a Symmetric key cipher

Several approaches to challenge-response authentication use symmetric-key encryption. The secret shared key, which is known to both claimant and the verifier. An encrypting algorithm is applied on the challenge.

- In the first approach, the verifier sends a nonce, a random number used only once to challenge the claimant. A nonce must be time varying, everytime it is created, it is different.

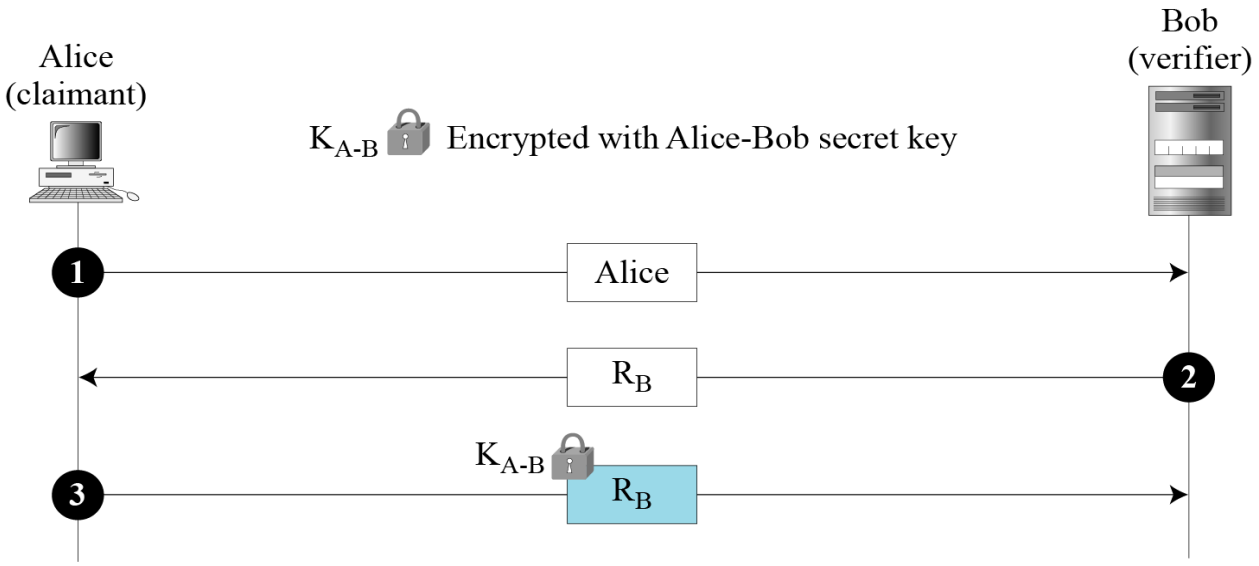


Fig.1.3 Nonce challenge

- In the second approach, we find that the time-varying value is a timestamp, which continues to vary with time. Challenge message here is the current time sent by the verifier to the claimant.

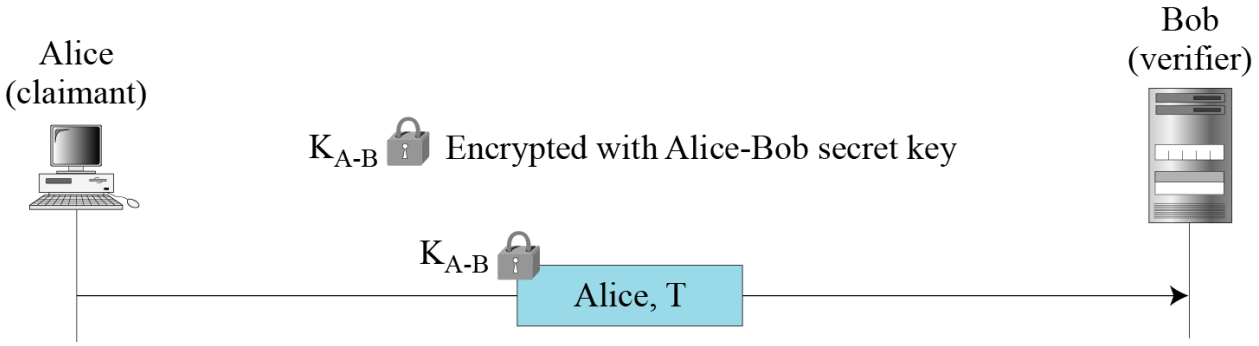


Fig. 1.4 Timestamp challenge

- 1st and 2nd approaches are for unidirectional authentication. If Alice also needs to be sure of the Bob's identity this approach is used.

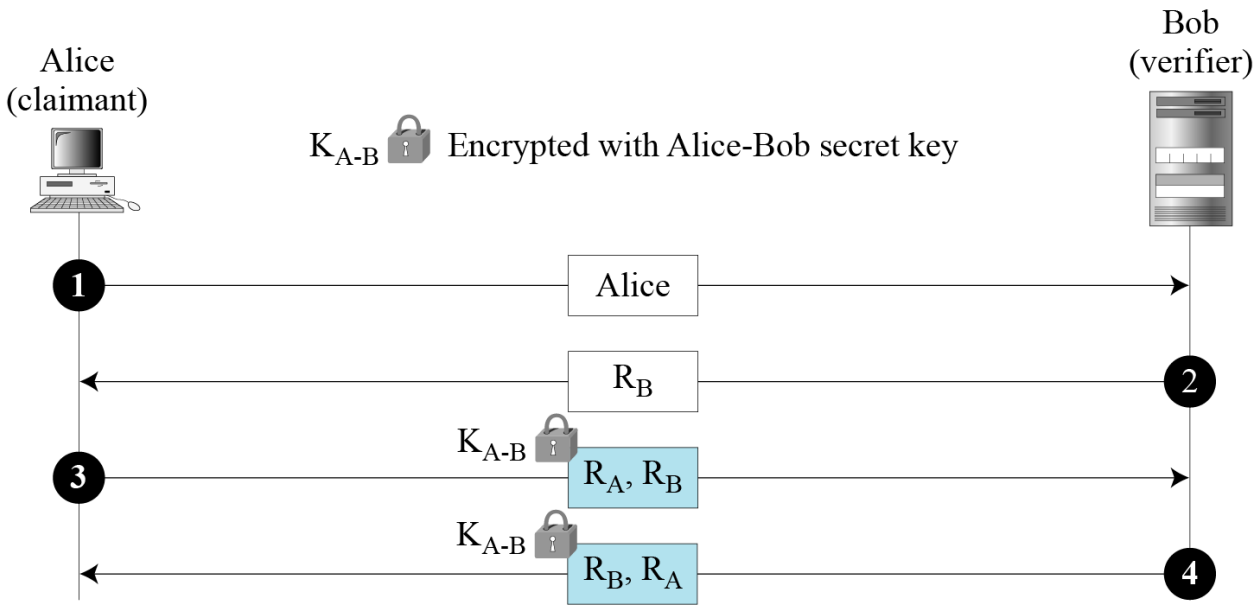


Fig.1.5 Bidirectional authentication

1.2.2.2 Using a Keyed hash functions

Here we basically use a keyed-hash function (MAC). It has the advantage of preserving the identity.

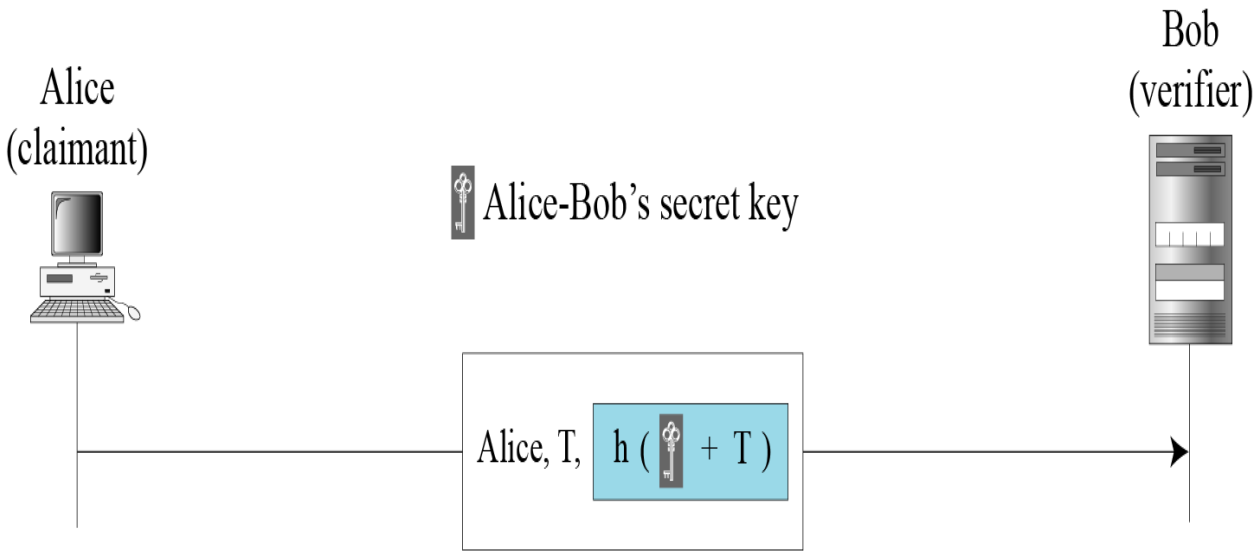


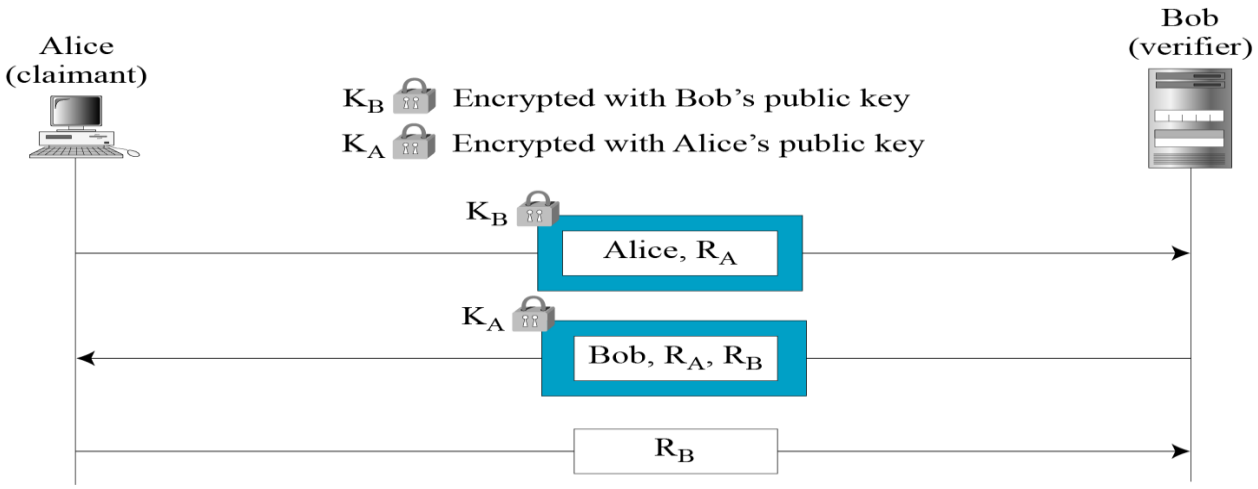
Fig.1.6 Keyed-hash function

1.2.2.3 Using Asymmetric key Cipher

Here the private key used by the claimant is the part of the secret. The claimant has to show that he/she has the private key, which is related to the public key which everyone has access to.

- First approach is used where verifier encrypts the challenge by using claimant's private key. Then the claimant can decrypt the message by using its secret key and sends a timestamp (nonce). In the second approach, two public keys are used each in one direction.

- In the second approach, two public keys are used each in one direction



- Fig.1.7 Bidirectional, asymmetric key

1.2.2.4 Using Digital Signature

Entity authentication can also be achieved by using a digital signature. When a digital signature is used for entity authentication, the claimant uses her private key for signing.

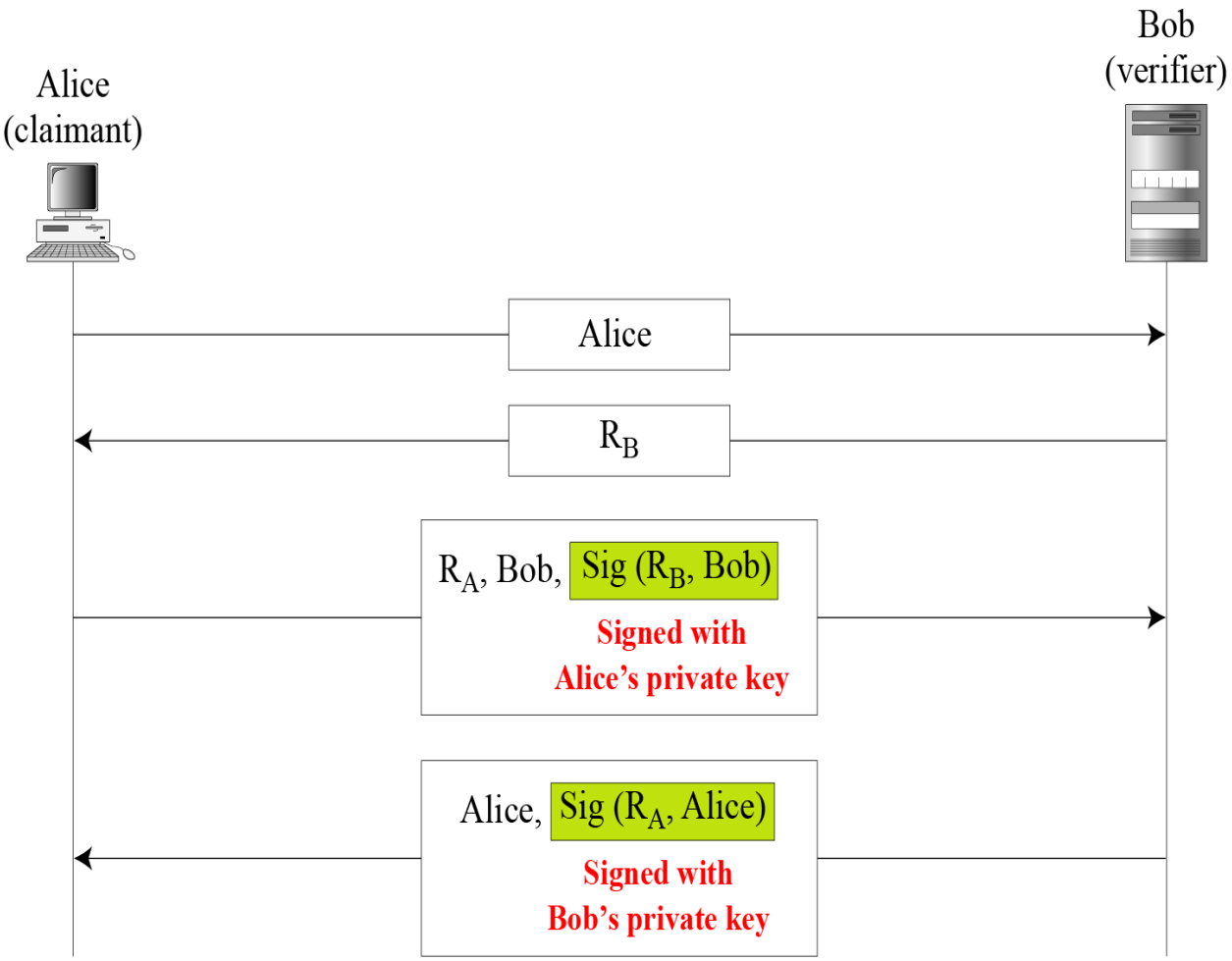


Fig.1.8 Bidirectional authentication

1.2.3 Zero Knowledge Authentication

In Cryptography, the Zero Knowledge confirmation/convention is a sort of convention in which one entity (claimant) demonstrates an alternate entity (verifier) that a certain information is genuine separated from the way that it doesn't pass on that the data given is genuine or false.

If to demonstrate the proclamation we require some data from the claimant, then the verifier can't take care of the issue on the grounds that it doesn't have the data. On the off chance that the information tells that the claimant just has the mystery data, it turns into an uncommon case known as zero-learning verification strategy. It demonstrates that learning of given data is vital if one is permitted to uncover that data; the test demonstrates that one has notable information even without uncovering the mystery.

For zero-information strategy, the protocol need to have intuitive data from the verifier, for the most part as a test, so that the reactions from the inquirer will have the verifier persuaded that if and if the articulation is genuine (i.e., if the petitioner to be sure has some guaranteed learning). This is the situation, since in the other case the verifier can record it and replay it someplace else. In the event that this were to be acknowledged by the late gathering as evidence that the replaying gathering surely has some information about the mystery data, then the acknowledgement of the new gathering could be defended as the verifier has learning about the mystery data.

Chapter 2

Literature Survey

A Zero-knowledge technique must satisfy three conditions:

1. **Completeness**: if this statement is true, the honest verifier will always be convinced of this fact by an honest claimant.
2. **Soundness**: If the statement provided by the claimant is false, no cheating claimant will be able to convince the honest verifier that it is actually true.
3. **Zero-knowledge**: If the statement is true, no cheating verifier can learn anything other than this property. This is proved by showing that every cheating verifier has some simulator that can give a fake transcript of interaction between the claimant and the verifier when it has to prove about the relationship.

.

Zero knowledge evidences are not proofs in the scientific feeling of the term on the grounds that there is some little likelihood, the soundness mistake, that a swindling petitioner will have the capacity to persuade the verifier of a false proclamation. At the end of the day, zero-information evidences are probabilistic "confirmations" as opposed to deterministic verifications. Be that as it may, there are systems to diminish the soundness lapse to irrelevantly little values.

A formal meaning of zero-information need to utilize some computational model, that of a Turing machine. Let P, V, and S be turing machines. An intelligent evidence framework with for a dialect is zero-information if for any probabilistic polynomial time (PPT) verifier there exists a normal PPT test system such that

$$\forall x \in L, z \in \{0,1\}^*, \text{View}_{\hat{V}}[P(x) \leftrightarrow \hat{V}(x,z)] = S(x,z)$$

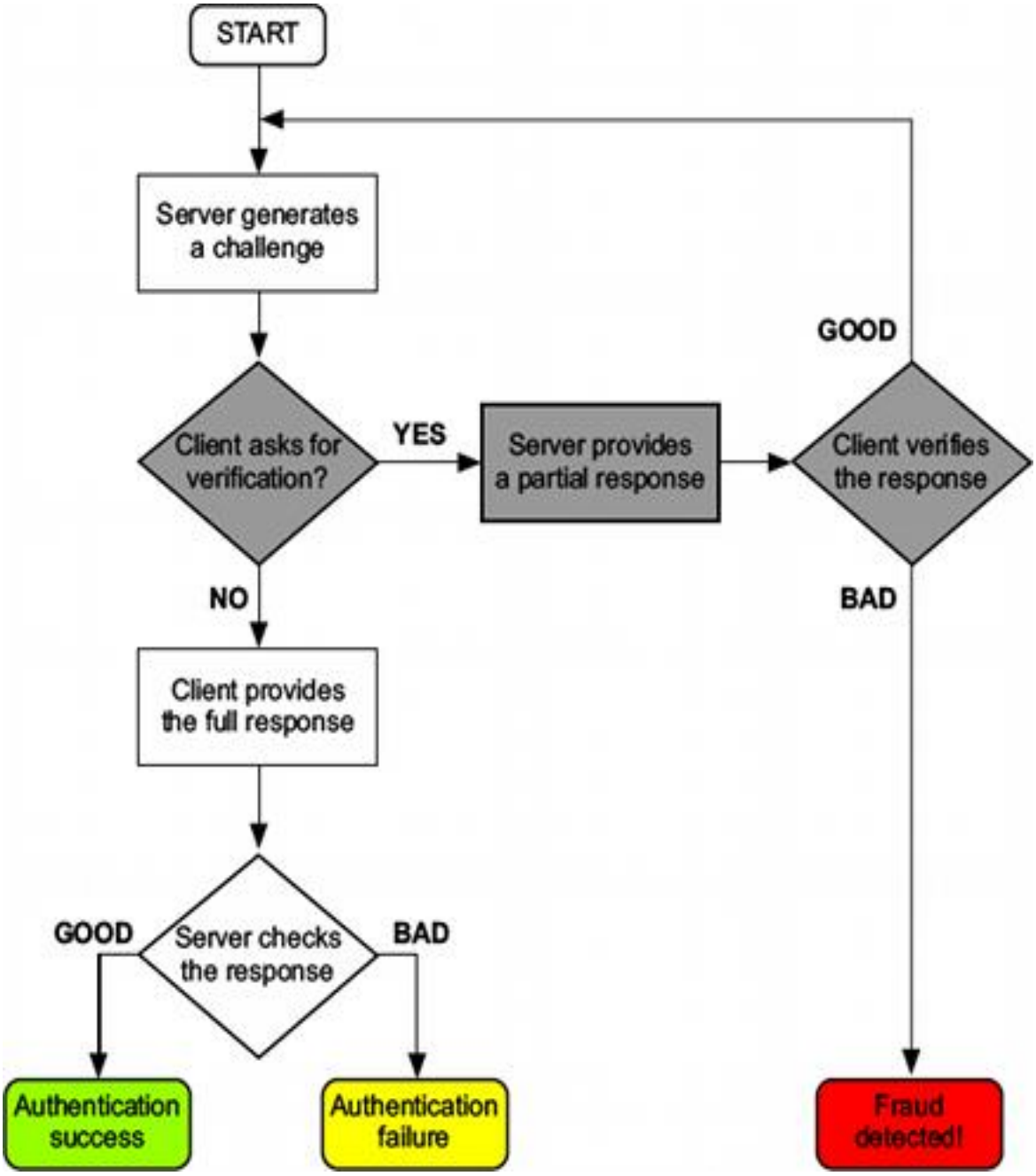


Fig. 2.1 Basic zero knowledge scheme

There are basically 3 protocols for implementing the Zero- Knowledge protocol.

1. Fiat-Shamir Protocol
2. Feige-Fiat-Shamir Protocol
3. Guillou-Quisquater Protocol

2.1 Fiat-Shamir Protocol

In the Fiat-Shamir convention, a trusted outsider picks two vast prime numbers p and q to ascertain the quality of n=p*q. The quality of n is affirmed to general society; the qualities of p and q are kept mystery. Alice the inquirer picks a mystery number s between 1 and n-1. She ascertains v=s2 mod n. She keeps s as her private key and registers v as her open key with the outsider. Confirmation of Alice by Bob is possible in four steps.

1. Alice, the Claimant picks a number between 0 to n-1, and r being called the commitment. She can evaluate the value of $x=r^2$ mod n; and name the value of x as witness.
2. The value of x is sent to Bob by Alice as witness.
3. Then Bob sends a value of c, which is called as the commitment. It can be either 0or 1.
4. Alice evaluates the response $y=r\ s^c$. Here r, s, c carry their usual meaning.
5. Alice sends the value of response y and claims to be Alice.
6. Bob calculates y^2 and $x\ v^c$ .If these two values are congruent, then Bob can conclude that Alice either knows the value of the secret key or he has guesses the value of y in some other dishonest ways.

$$\mathbf{Y^{2=}\ (r\ s^c)\ ^2=r^2\ s^{2c}=r^2\ (s^2)\ ^c=x\ v^c}$$

2.2 Feige -Fiat-Shamir Protocol

The Feige -Fiat-Shamir convention is like the first approach aside from it utilizes a vector of private keys [s_1, s_2… .,s_k] , a vector of open keys [v_1, v_2,… ..v_k] and a vector of difficulties (c_1, c_2… .c_k). The private keys are picked arbitrarily, yet they must be relatively prime to n. People in general keys are picked such that

$$V_i = (S_i^{\,2})^{-1} \bmod n$$

We have to prove that $y^2 v_1^{c1} v_2^{c2}$……is congruent to x.

2.3 Guillou- Quisquater Protocol

The Guillou-Quisquater Protocol is a growth of Fiat-Shamir convention in which fewer rounds could be utilized to demonstrate the personality of the petitioner. A trusted outsider picks two prime numbers p and 1 to compute the worth of n=p*q. The trusted gathering likewise declares the example e, which is co-prime with φ=(p-1)(q-1). The qualities of n and e are advertised to people in general while the worth of p and q are kept mystery. The trusted gathering picks two numbers for every element, v which is open and s which is private. However for this situation, the relationship between v and s are distinctive.

$$S^e * v = 1 \bmod n$$

The three exchanges constitute a round; verification is repeated several times with a random value c between 1 and e. the claimant has to pass the test in every round to get verified. If she fails a single round, then the process is aborted and she is not authenticated.

$$y^e v^c = (r\, s^c)^{\,e} v^c = r^e * s^{ce} * v^c = r^e (s^e v)^c = x(1)^c = x$$

Chapter 3

3.1 Implementation

3.1.1 Fiat-Shamir Protocol

$$y^2 = (rs^c)^2 = r^2 s^{2c} = r^2 (s^2)^c = xv^c$$

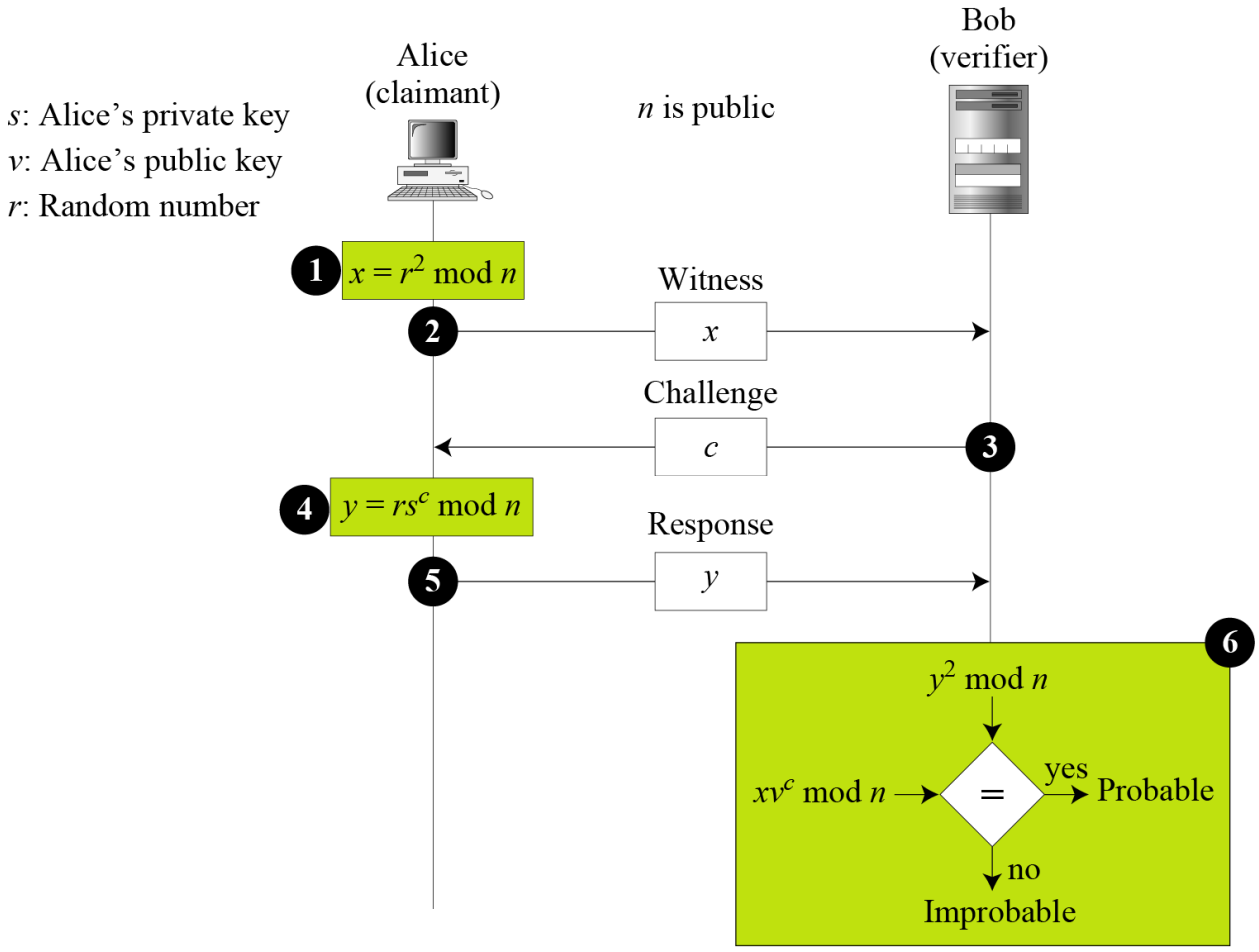


Fig.3.1 Fiat-Shamir Protocol Scheme

As we know according to this protocol, it is verified with different value of c and the claimant has to pass all round to verify itself. Failing to one single round, the process is aborted.

- As we know Alice can be honest or dishonest. By being honest he can pass each round and if she is not honest, if she can guess all values of challenges, then also she can pass every round.
- If she is dishonest and she guesses that the value of c is 1, she may evaluate the value of $x=r^2/v$ and thus can send x to be the witness.
    1. If she guessed it correctly, then she will send y=r as her response.
    2. If she is wrong, a value which will pass the test can't be found, thus the process will be aborted by Bob.

- Then if Alice guesses that c is 0, she may evaluate the value of $x=r^2$ and x will be sent as a witness.
    1. If she guessed it correctly, then y=r will be sent as response.
    2. If she is wrong, then the process will abort.

Thus we can easily find that the verifier has 50% chance to fool the claimant. If this process is repeated many times, then the chance of claimant deceiving the verifier will reduce by a great margin.

.

Ali Baba Cave Problem

Suppose there is a underground cave like the below cave with a door at both end which will open with some magic word. Alice says that she knows the word and thus can open the door. Suppose both Alice and Bob are standing at the entrance point A, then Alice goes to B, where Bob can't see Alice.

- Alice can move to either right or left and it can be corresponded to the witness.
- Then Bob comes to B and asks Alice to come from left or right and thus it corresponds to challenge.
- If Alice knows the word, she can come from any side which is requested. Because if she is on the right side, she can come easily and if on the wrong side, she can use the magic word to come from the requested side.
- This game can be repeated many times, Alice can win the game if she can pass the test all the time. The probability of her winning the game is very less if doesn't have the private key (word).

So if the game is run N times and as each time Alice has ½ chance of winnig.so the chance of Alice winning the game is $(1/2)^N$.

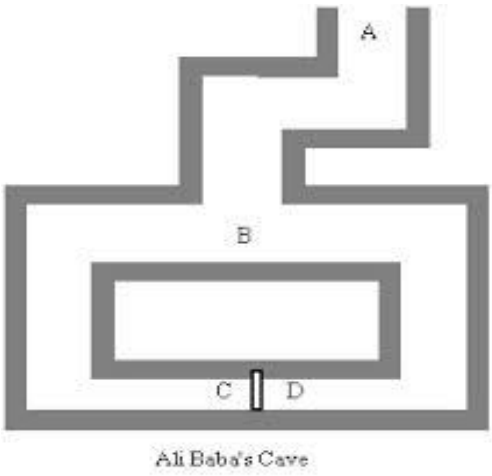


Fig.3.2 Ali Baba Cave

3.1.2 Fiege-Fiat-Shamir Protocol

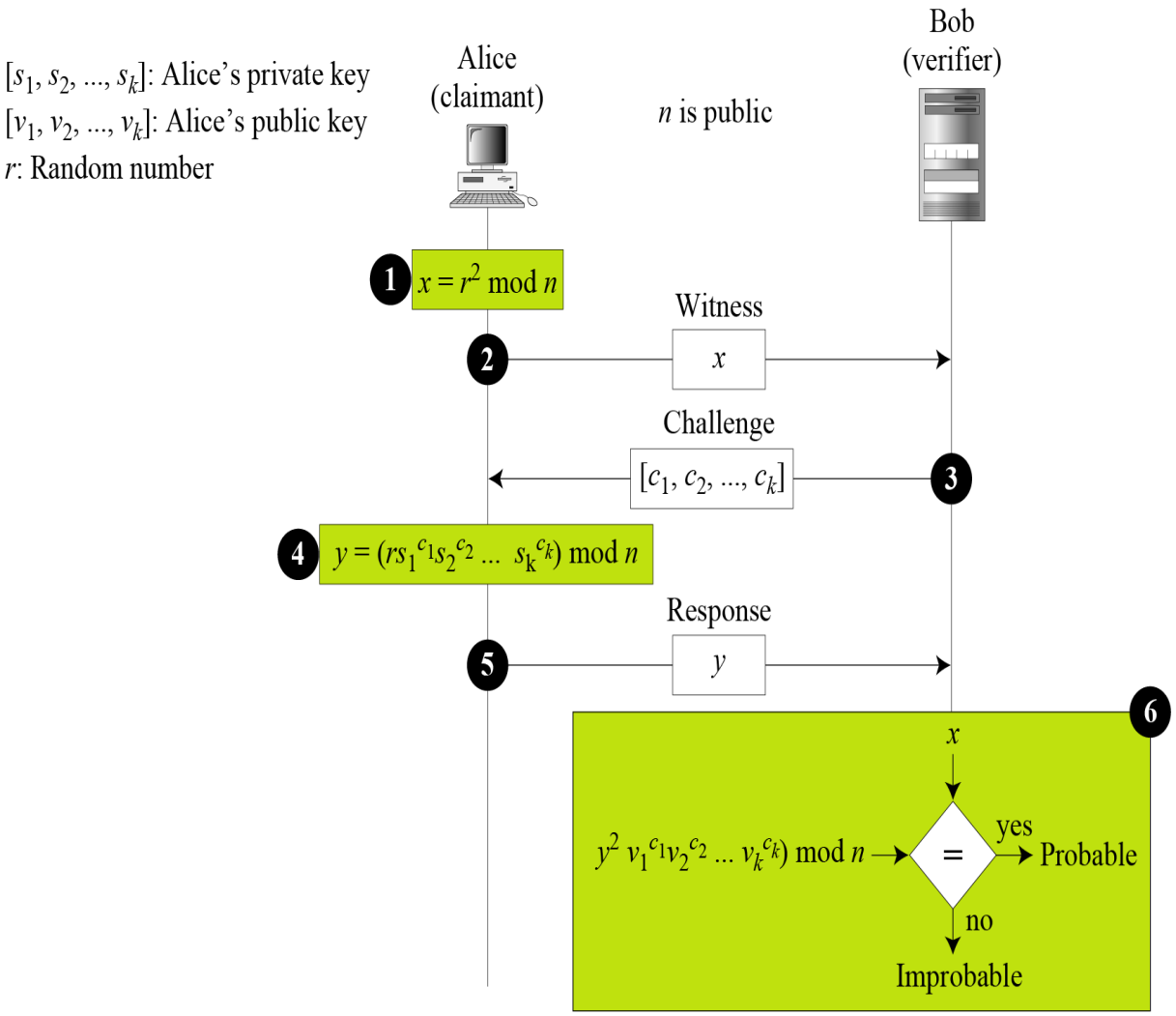


Fig.3.3 Fiege-Fiat-Shamir Protocol Scheme

$$y^2 v_1^{c_1} v_2^{c_2} \cdots v_k^{c_k} = r^2 (s_1^{c_1})^2 (s_2^{c_2})^2 \cdots (s_k^{c_k})^2 v_1^{c_1} v_2^{c_2} \cdots v_k^{c_k}$$
$$= x(s_1^2)^{c_1}(v_1^{c_1})(s_2^2)^{c_2}(v_2^{c_2}) \cdots (s_k^2)^{c_k}(v_k^{c_k})$$
$$= x(s_1^2 v_1)^{c_1}(s_2^2 v_2)^{c_2} \cdots (s_k^2 v_k)^{c_k}$$
$$= x(1)^{c_1}(1)^{c_2} \cdots (1)^{c_k} = x$$

3.1.3 Guillou-Quisquater Protocol

- By performing a series of verification experiment, it is possible to prove that you know a certain secret without sharing it with anyone.
- Zero-Knowledge Protocols help prevent leaks of any secret information by not directly requesting the secret itself during verification.
- Zero-Knowledge Protocols won't care if you actually know the password or not, as long as you can prove that you know it.
- Faking the proof of knowing the secret is possible, but it has a low probability of success.
- It is an extension of Fiat-Shamir Protocol.

$$y^e \times v^c = (r \times s^c)^e \times v^c = r^e \times s^{ce} \times v^c$$

$$= r^e \times (s^e \times v)^c = x \times 1^c = x$$

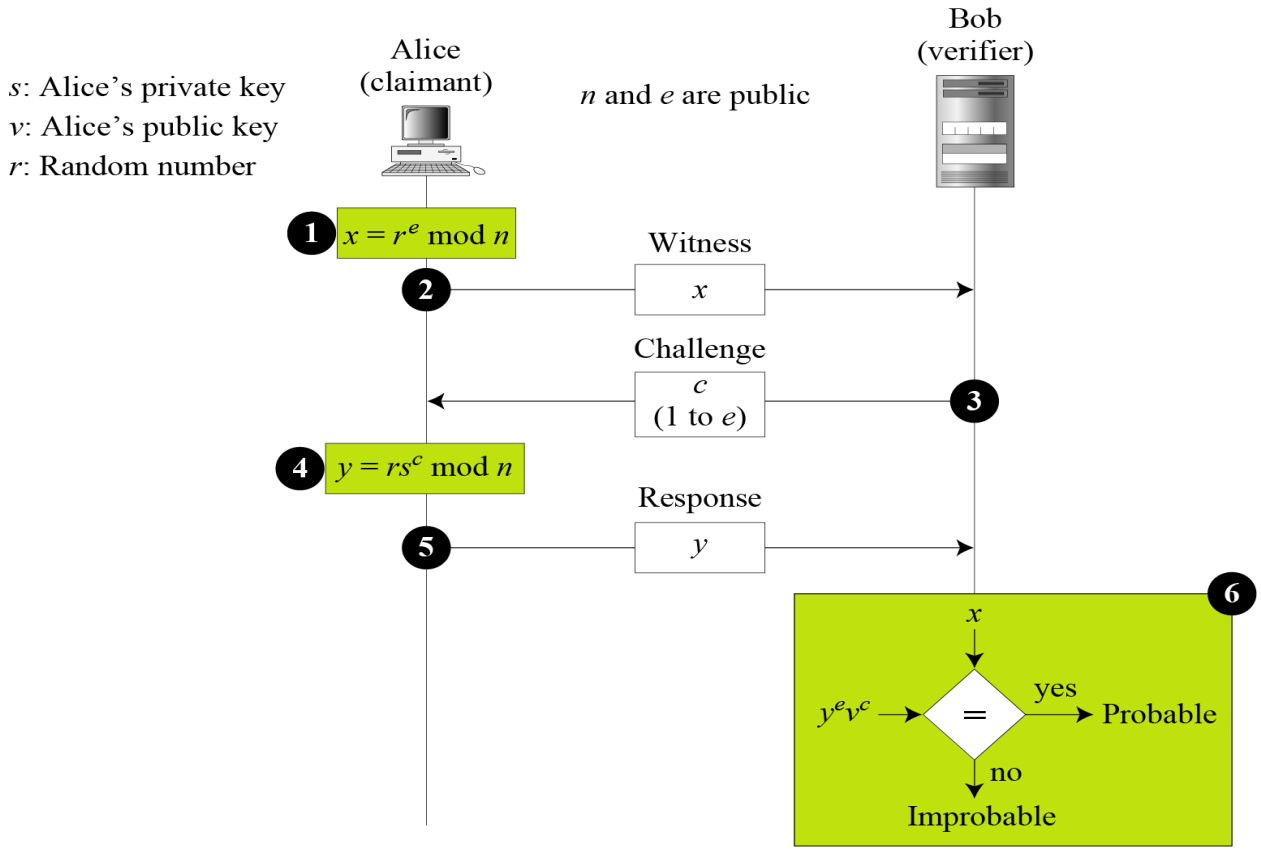


Fig.3.4 Guillou-Quisquater Algorithm

3.2 Real World Applications

1. Network Authentications
2. Smart Cards
3. Key Exchanges
4. Digital Signatures

3.3 Advantages and Disadvantages of Zero Knowledge Authentication

Advantages of Zero-Knowledge Protocols:

- Secured – It doesn't require someone to reveal secret..
- Simple – Critical encryption methods are not necessary..

Disadvantages of Zero-Knowledge Protocols:

- Limited – Translation might be necessary if secret is not a number.
- Lengthy – As it has almost 2k entity, it takes a lot of time to compute.
- Imperfect – The Intruder can still intercept the message (i.e. messages to the Verifier might be modified or destroyed).

3.4 Results

3.4.1Fiat-Shamir Protocol

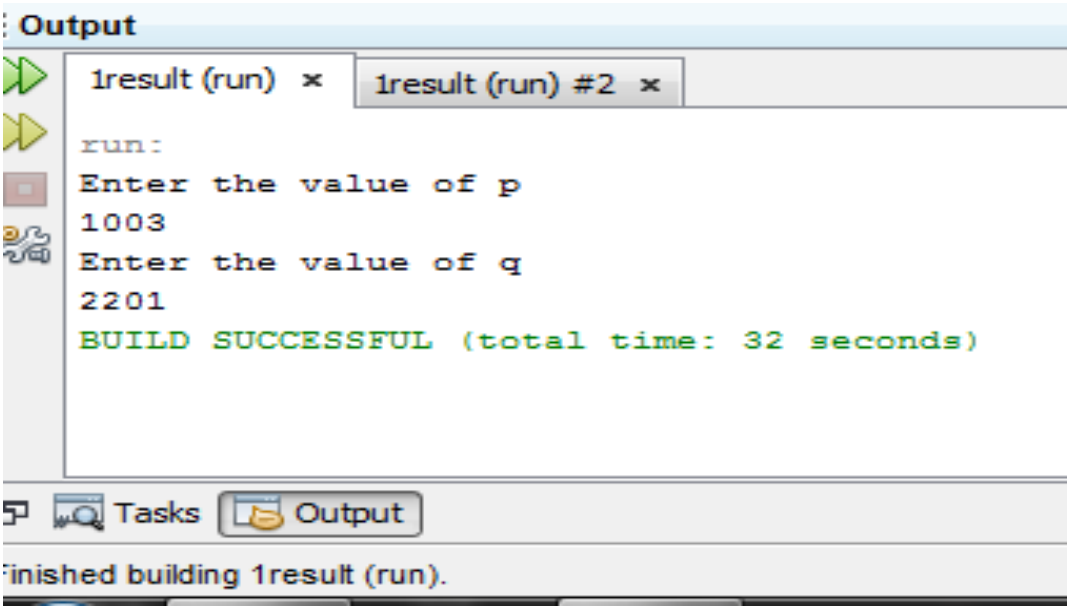


Fig.3.5 Fiat-Shamir Server side

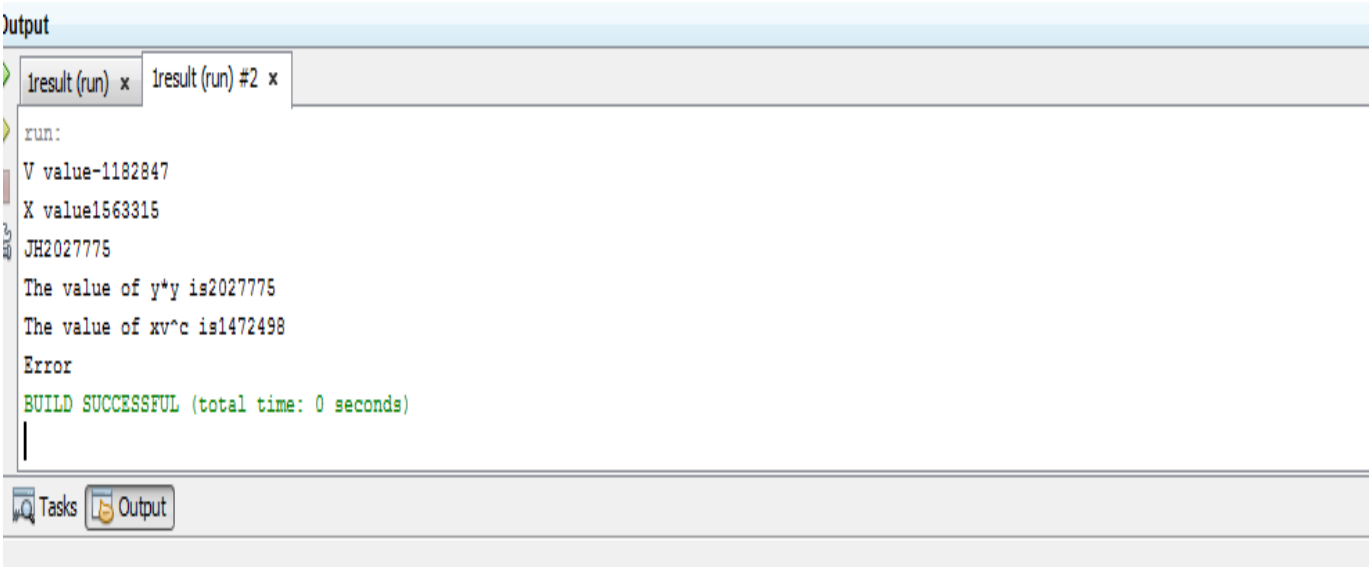


Fig.3.6 Fiat-Shamir Client side

3.4.2 Fiege-Fiat-Shamir Protocol

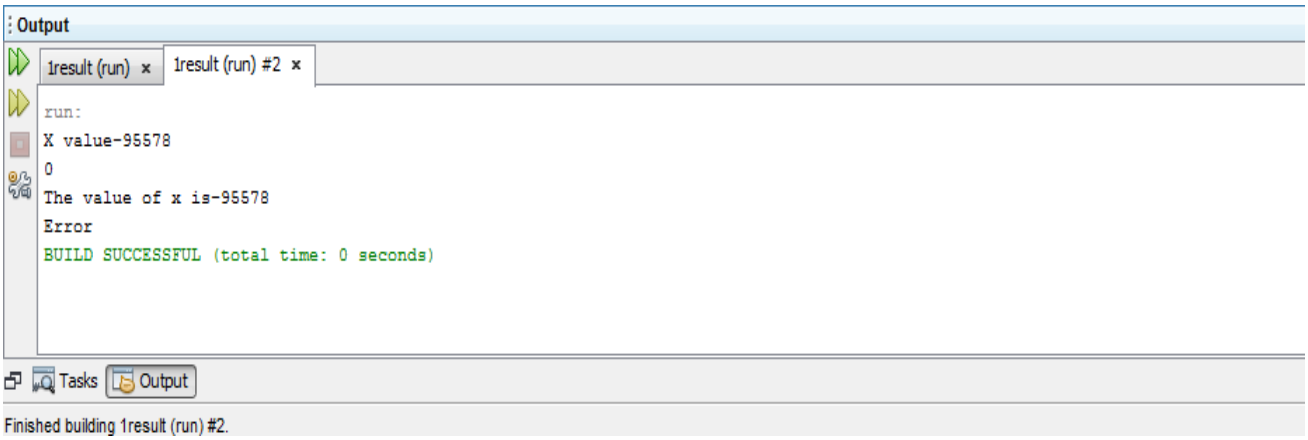


Fig.3.7 Feige-Fiat-Shamir Client side

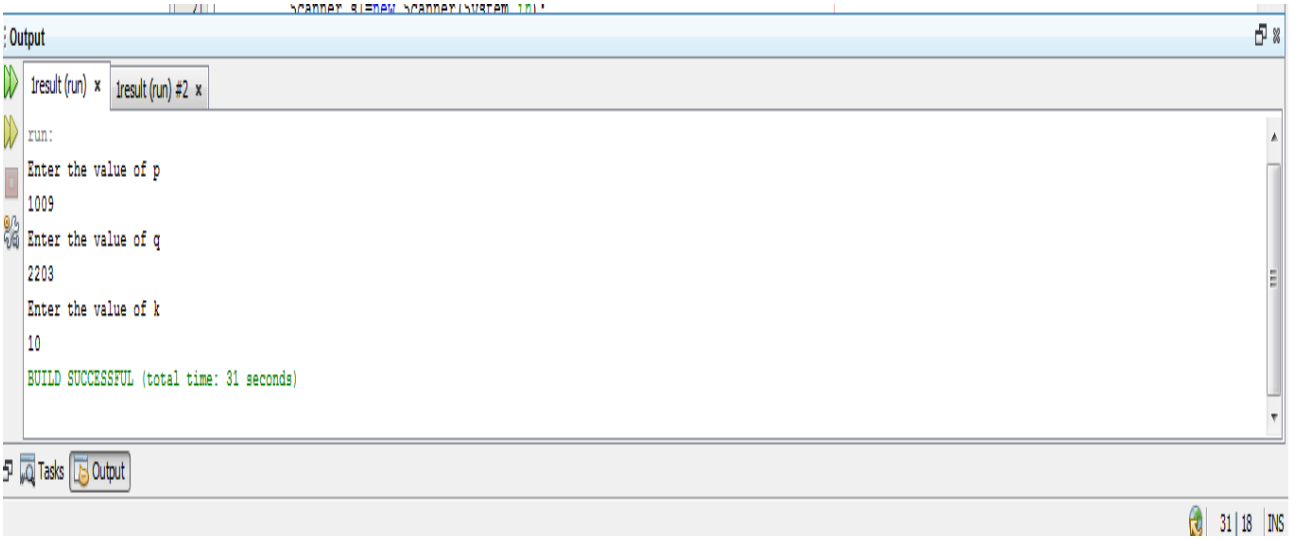


Fig.3.8 Feige-Fiat-Shamir Server side

3.4.3 Guillou-Quisquater Protocol

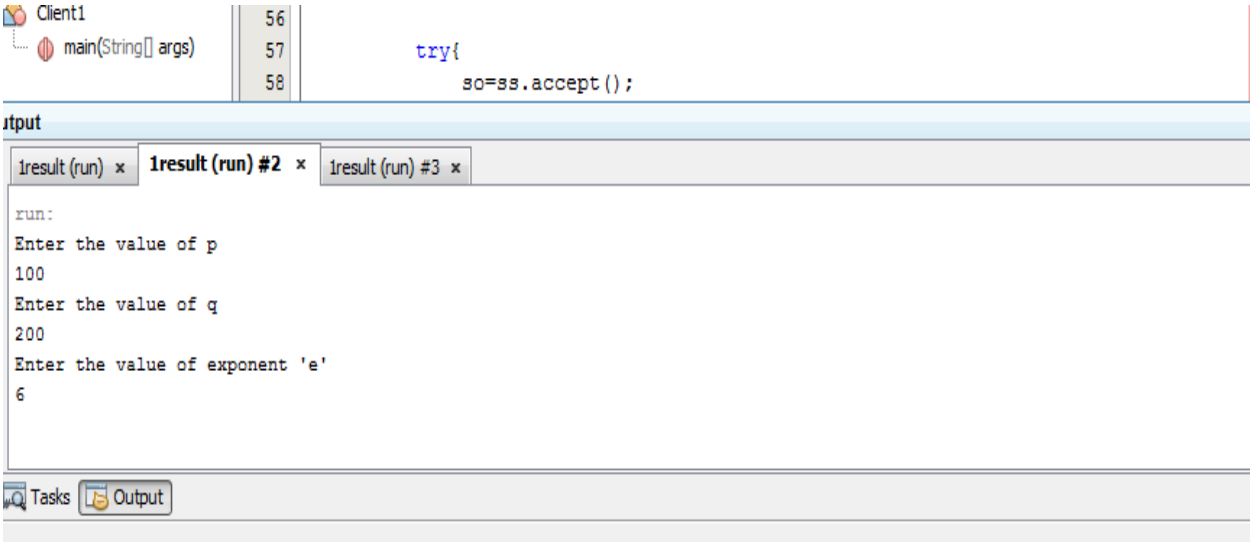


Fig.3.9 Guillou-Quisquater Server side

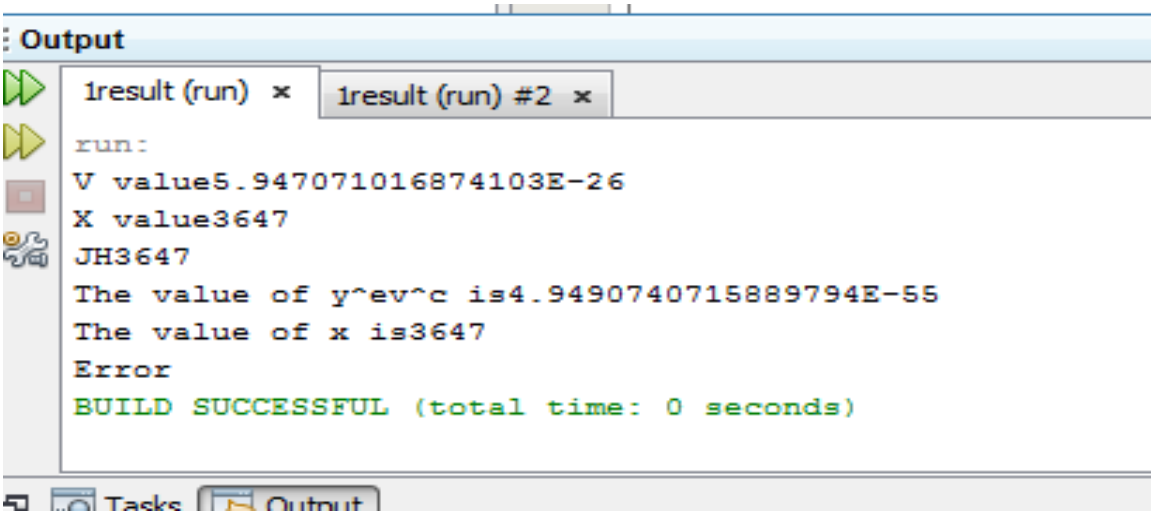


Fig.3.10 Guillou-Quisquater Client side

Chapter 4

Analysis

4.1 Security Analysis

The security of the first Fiat-Shamir plot fundamentally might be centered around the way that discovering the square foundations of irregular v_j qualities is truly troublesome as the factorization of the modulus. The new procedure can't straightforwardly pertinent to the new form, as the extraction of square bases of little primes may be less demanding than discovering those of the arbitrary numbers.

For straightforwardness purpose, we think just the security of the distinguishing proof plan (the mark plan may require a more particular result), the ID conspire being referred to being focused around zero-learning evidences. This implies that the verification of character is constituted by an evidence of "learning of something." Since the gatherings execute stand out round of the convention, the petitioner can succeed with likelihood 1/2 regardless of the possibility that all the primes are quadratic non-deposits! Essentially, the convention is not an evidence of learning of square roots (either for a specific prime or for all the primes).

The information tape could discover the square bases of 11 the 400 Pair savvy results of the primes, and in this way a smart claimant could persuade the verifier with likelihood 1/2 without really knowing even one of the first roots.

This is worth specifying that while such a presumption is sufficient to demonstrate the security of the new plan, it for the most part doesn't surmise that our plan is frail! Actually, regardless of the possibility that a swindling verifier knows how to element n by utilizing the square foundations of a little number of little primes, he is unrealistic to get hold of these square roots since the plans are the parallel renditions of zero learning conventions.

4.2 Attacks

Here are some attacks which are used to mainly break the Zero Knowledge techniques.

- Impersonation
- Replay
- Interleaving
- Reflection
- Forced Delay
- Chosen-text

- Impersonation is the act of pretending of an entity.
- Replay attack utilizes an impersonation involving use of information from an already used protocol repeatedly on the verifier.
- An impersonation which involves a certain combination of information from previous protocols executions is called as an interleaving attack.
- Reflection is an interleaving attack which involves sending information from an ongoing protocol execution to the original entity.
- An adversary when it intercepts a message and uses it in the later stages is using a forced delay attack.
- And finally, a chosen-text attack is when an adversary chooses specific challenges for gaining information about the secret or private key.

Chapter 5

Conclusion

Zero-Knowledge conventions permit the verifier to demonstrate to the verifier that they know a mystery without uncovering data about that mystery. By thinking about qualities between the dedication and reaction, the verifier can ascertain whether the reaction matches the normal worth. This permits the verifier to check data without having any learning of s, the mystery private to the verifier. This procedure might be utilized to permit unnamed confirmation in gadgets, for example, RFID labels. Particularly where protection of mystery data is at a premium, for example, travel permits, RFID labels with a Zero Knowledge convention could be utilized to ensure particular data while as of now being utilized to verifier the validness of the individual with the passport.

Bibiliography

[1] B. Schneier, "Applied cryptography", John Wiley and Sons,1994.

[2] T. Beth, and Y. Desmedt, "Identification Token-or: Solving the Chess Grandmaster problem", Advances in cryptology crypto' 90, LNCS 537, pp. 169-176,1991.

[3] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems.", Siam J. Compute, 18(1), pp. 186-208, February 1989.

4] J. Brandt, I. B. Damgard, P. Landrock, and T. Pedersen. Zero-Knowledge Authentication Scheme with Secret Key Exchange. In Proceedings of *Advances in Cryptology*, 1990.

[5] G. J. Simmons and G. B. Purdy. Zero-Knowledge Proofs of Identity and Veracity of Transaction Receipts. In Proceedings of EUROCRYPT,

[6] L. Lu, Y. Liu, L. Hu, J. Han, and L. M. Ni. Pseudo Trust: Zero-Knowledge Authentication in Anonymous Peer-to-Peer Protocols.

[7] U. Fiege, A. Fiat, and A. Shamir. Zero Knowledge Proofs of Identity. In Proceedings of *ACM Symposium on Theory of Computing(STOC)*, 1987.

[8] Alfred J Menezes, Paul C. van Oorschot, Scott A. Vanstone *Handbook of Applied Cryptography*.

[9] Behrouz A. Forouzan, Debdeep Mukhopadhay in *Cryptography and Network Security*.

[10] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, “Strong authentication for RFID aystems using the AES algorithm,” in *Proc. Cryptogr.Hardw. Embed. Syst., CHES’04*, 2004, vol. 3156, LNCS, pp. 357–370.

[11] S. I. Ahamed, F. Rahman, “ERAP: ECC based RFID authentication protocol,” in *Proc. 12th IEEE Int. Workshop on Future Trends of Distrib. Comput. Syst. (FTDCS’08)*, 2008, pp. 219–225.

[12] K. Peng and F. Bao, “Efficient publicly verifiable secret sharing withcorrectness, soundness and ZK privacy,” *Inf. Secur. Appl.*, vol. 5932, pp. 118–132, 2009.